UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/593,280	06/13/2000	Cheuk W. Ko	NA00-02401	7783

28875 7590 07/26/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENEGHAN, MATTHEW E	

ART UNIT	PAPER NUMBER
2134	13

DATE MAILED: 07/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/593,280
Filing Date: June 13, 2000
Appellant(s): KO, CHEUK W.

Kevin J. Zilka
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 30 April 2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The appellant's statement in the brief that certain claims do not stand or fall together is not agreed with because claim 7 is listed as belong to both Issue #1, Group #1 and Issue #1, Group #3.

It is being presumed in this Examiner's Answer that claim 7 belongs to Issue #1, Group #3.

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

4,713,754	Agarwal	12-1987
5,513,317	Borchardt et al.	4-1996
5,557,742	Smaha et al.	9-1996
5,623,601	Vu	4-1997

6,584,508 Epstein et al. 6-2003

Kernighan et al., "The UNIX Programming Environment," 1984, pp. 174 and 201-217.

Microsoft Computer Dictionary, 5th Edition, pp. 42, 166, 264, 285, 286, 300, and 343.

(10) Grounds of Rejection

The following grounds of rejection are applicable to the appealed claims:

Claims 1-27 are rejected under 35 U.S.C. 103(a). This rejection is set forth in a prior Office Action, mailed on 10 February 2004.

Regarding claim 1, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al. (hereinafter "Smaha") in view of U.S. Patent No. 5,513,317 to Borchardt et al. (hereinafter "Borchardt").

As per the first limitation of claim 1, the first limitation is anticipated by the receipt of inputs from the "selected misuse input mechanism 20," which specifies the attributes to be audited (see column 9, lines 40-41).

As per the second limitation, the "signature data structure" specifies one or more target attributes to be recorded, and embodies a specification of what constitutes a "misuse." The set of attributes to be retrieved into the structure is defined by the structure, and is a subset of the elements available for collection on the system (see column 8, lines 8-46).

As per the third limitation, the misuses are selected from a maximum set of all misuses (see column 8, lines 63-66), thus specifying at least one auditing criterion from a set (see column 9, lines 41-47).

The functionalities of the second and third limitations are both performed during the auditing process (see column 9, lines 37-45).

As per the fourth limitation, an event that is found by comparing the signature data structures to the sets of misuses are produced when the engine reaches an "end state." This produces an output to the output report mechanism 42, which constitutes the recording of the target attribute (see column 7, lines 8-49 and column 10, lines 41-45).

As per the fifth limitation, the output report mechanism 42 constitutes an "audit log," moreover, several means that would constitute such an audit log are disclosed in column 10, line 55 to column 11, line 23 and figures 6a and 6b.

Regarding the sixth limitation, the purpose of Smaha's entire invention is to allow a user to automatically recognize intrusions and misuses (see column 3, lines 5-11), and the produced output reports are examined for intrusion detection purposes (see column 3, lines 30-36). Moreover, Smaha specifically states the examination of the logs for patterns via statistical analysis (see column 11, line 2).

Regarding the seventh and final limitation, it is presumed from Appellant's specification that the size of the output is reduced in size as a result of the fact that data not delineated in the audit specification are discarded (see Appellant's specification, p. 11, lines 1-5); in other words, the author of the audit specification

deliberately chooses a specification that produces the filtering out of some data. Though it is disclosed that Smaha's invention is used to reduce the number of false misuses reported (see column 3, lines 45-53), Smaha does not disclose the deliberate reduction of the size of the audit log prior to examination.

Borchardt discloses a trace filter in which data is deliberately filtered according to one or more attributes before being analyzed by the programmer (see column 4, lines 1-19), and suggests that the volume of information provided by a trace facility can grow to such large proportions as to obscure the few relevant pieces of information that the trace facility has captured (see column 1, lines 56-59).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Smaha by deliberately filtering according to one or more attributes before being analysis, as disclosed by Borchardt, as the volume of information provided by a trace facility can grow to such large proportions as to obscure the few relevant pieces of information that the trace facility has captured.

Claims 2, 8-12, 17-20, 26, and 27 stand or fall with claim 1.

Regarding claim 3, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al. in view of U.S. Patent No. 5,513,317 to Borchardt et al.

Smaha discloses that the signature information structure is initialized in a UNIX® system by retrieving it from disk storage (see column 12, lines 5-40). All

transactions with disk storage in the UNIX® operating system are necessarily performed using one of a number of system calls, such as read(), open(), and close().

Smaha does not specifically disclose the use of jump tables for choosing the appropriate system calls for performing file I/O.

Official notice has been given that it is well-known in the art that the method of using a jump table is an efficient way, both in terms of execution speed and memory usage, to specify a jump or call to one of a list of processes in a situation where the decision can be made based upon the value of an single integer variable, such as an index, and that jump tables can be dynamically modified, based upon changing conditions, as shown by Agarwal (see Agarwal, figure 4, items 406 and 408 and column 8, lines 6-26, especially lines 6-12).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Smaha by using a system call jump table, in order to efficiently choose the correct system call by which to retrieve the signature information structure from disk storage.

Claims 13 and 21 stand or fall with claim 3.

Regarding claim 7, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al in view of U.S. Patent No. 5,513,317 to Borchardt et al.

The filtering of at least one target attribute was disclosed in the rejection of base claim 1. The filtering of data from an audit log reduces the amount of data stored in it, as the removal of data from files always makes them smaller.

Claims 16 and 25 stand or fall with claim 7.

Regarding claim 4, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al in view of U.S. Patent No. 5,513,317 to Borchardt et al. in view of U.S. Patent No. 6,584,508 to Epstein et al. further in view of Kernighan et al., "The UNIX Programming Environment," 1984 (hereinafter "Kernighan").

Smaha discloses the analysis system level events (i.e. system calls) in the misuse engine (see column 9, lines 65-67), but does not specifically detail how it is done. The issue is outside the scope of Borchardt.

The data guard system disclosed by Epstein includes the ability to screen a variety of system call attributes by using wrappers around system calls, so that any parameter to the system call may be intercepted (see column 5, lines 32-55). Epstein further discloses that intercepted calls might include an exec call, for which the name of a process is passed as a parameter, or an attempt to read a file, for which a parameter must be an identifier for the calling application program (see column 6, lines 58-67). Epstein further suggests that the software wrappers provide for relatively small specifications of the allowed behavior of associated multi-part proxy components, and security of firewall components is thereby improved (see column 3, lines 29-32).

Epstein does not completely detail the attributes that are included in system calls, but states that all system calls may be intercepted, along with all associated parameters ("arguments").

Kernighan discloses that systems calls may contain information about the process making the system call, from argv[] (see pp. 174 and 217) or the file descriptor or the data buffer for reading or writing (see p. 202). Since all peripheral devices use file descriptors in system calls (see p. 201) and UNIX is a network operating system used on computers wherein peripherals (such as Ethernet cards) are used for network communications, it is inherent that parameters may also be related to network communications.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the intrusion detection system disclosed by Smaha and Borchardt by implementing software wrappers for the system calls, making the parameters of system calls available for auditing, as disclosed by Epstein, screening all UNIX system call parameters disclosed by Kernighan, thereby improving the security of firewall components.

Claims 13 and 22 stand or fall with claim 4.

Regarding claim 6, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al in view of U.S. Patent No. 5,513,317 to Borchardt et al. in view of U.S. Patent No. 6,584,508 to Epstein et al. further in view of Kernighan et al., "The UNIX Programming Environment," 1984.

Smaha discloses the use of a UNIX® platform (see Smaha, column 7, lines 50-60), while Epstein states the auditing criteria can include a specific user or directory, which is a type of file (see Epstein, column 5, lines 56-60), or any other attribute extractable from system calls, but does not specifically specify the screening by the application from which the system call is being made.

Kernighan discloses that systems calls may contain information about the process making the system call, from argv[] (see pp. 174 and 217) or the file descriptor or the data buffer for reading or writing (see p. 202). Since all peripheral devices use file descriptors in system calls (see p. 201) and UNIX® is a network operating system used on computers wherein peripherals (such as Ethernet cards) are used for network communications, it is inherent that parameters may also be related to network communications.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the intrusion detection system disclosed by Smaha and Borchardt by implementing software wrappers for the system calls, making the parameters of system calls available for auditing, as disclosed by Epstein, screening all UNIX system call parameters disclosed by Kernighan, thereby improving the security of firewall components.

Claims 15 and 24 stand or fall with claim 6.

Regarding claim 5, the previously stated rejection is based upon U.S. Patent No. 5,557,742 to Smaha et al in view of U.S. Patent No. 5,513,317 to Borchardt et al. in view of U.S. Patent No. 5,623,601 to Vu (hereinafter "Vu").

Smaha and Borchardt do not disclose the incorporation of the misuse engine into the operating system's kernel, though the invention of Smaha is used for detecting system level events (see column 9, lines 65-67).

Vu discloses a system for secure gateway communications that includes the incorporation of the engine directly in the operating system kernel (see column 4, lines 51-64), and further notes that data communications are delivered to the application level through the kernel (see column 6, lines 2-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to incorporate the misuse engine disclosed by Smaha and Borchardt into the operating system kernel, as disclosed by Vu, as all data communications are delivered to the application level through the kernel.

Claims 14 and 23 stand or fall with claim 5.

(11) Response to Arguments

Regarding Appellant's arguments to Issue #1, Group #1 (claims 1, 2, 8-12, 17-20, 26, and 27) that Smaha does not contain an audit specification (see Appellant's Brief, pp. 6-7), it is noted that Appellant's specification only defines an audit specification in that it must have both target attributes and criteria (see Specification, p.3, lines 19-23).

The grounds of rejection stated above show that the invention disclosed by Smaha comprises both of the elements that comprise such a specification, the

misuse data itself and the signature data structure that is derived from the misuse data (see column 8, lines 11-17).

It is noted that the Microsoft Computer Dictionary, 5th Edition defines "auditing" as "The process an operating system uses to detect and record security-related events."

Regarding the definition of "misuse," for "misuse detection," the Microsoft Computer Dictionary, 5th Edition refers to the definition for "IDS," an intrusion detection system. An IDS is defined as "a type of security management system for computers and networks that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches."

It is therefore shown that the components disclosed by Smaha constitute the claimed audit specification, as both specify the data and method for analysis for the detection of security breaches.

Regarding Appellant's arguments that the selected misuses are not used to configure an audit system (see Appellant's Brief, pp. 7-8), it is noted that the set of misuses drives the misuse engine 30 (see figure 4), which then produces an output report 42 (see figure 1), which constitutes an audit log, as discussed above. Since Appellant's specification does not discuss the "detection of patterns," it is presumed that the sixth limitation refers to the application of the signature data (the patterns) as defined by the event data structure (the relevant elements extracted from the audit log) derived from by the list of misuses (the audit specification). Neither Appellant's specification nor Appellant's claims suggest that the audit specification and patterns must be independent of one

another; Smaha's system, wherein one is produced from the other, thus contains the cited limitations.

Regarding Appellant's argument that Appellant's invention is patentable over Smaha because Smaha does not disclose the "crux" of Appellant's invention, namely the reduction of recorded data (see Appellant's Brief, pp. 8-9), Smaha does not need to disclose anything over and above the invention as claimed in order to render it unpatentable. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim. In a claim drawn to a process of making, the intended use must result in a manipulative difference as compared to the prior art. See *In re Casey*, 152 USPQ 235 (CCPA 1967) and *In re Otto*, 136 USPQ 458, 459 (CCPA 1963).

It is also noted, moreover, that Smaha's disclosure does in fact suggest that that invention is used to decrease the number of false positive misuse reports (see column 3, lines 9-15); Appellant's specification similarly goes no farther than stating a general objective to support the claim for reducing the audit log size. Appellant's specification was, however, determined to be enabling with respect to this limitation because the filtering of data is so well-known in the art, as was noted in the first office action (see Paper No. 5, p.7, line 17 to p. 8, line 3), a point which Appellant has never attempted to argue. Nonetheless, a secondary reference, Borchardt, was incorporated into the final rejection, in view

of Appellant's amendment, with the intent of further establishing this particular feature's status within the art.

Therefore in response to Appellant's argument that Borchardt is nonanalogous art (see Appellant's Brief, pp. 9-12), it has been held that a prior art reference must either be in the field of Appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the Appellant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, it is an objective of the invention of Smaha that large amounts of data be processed into a manageable number of reports, as discussed above. Borchardt solves a corresponding problem, and, though Borchardt discloses an invention serving a different end purpose, the filtering strategy so disclosed can be directly applied to Smaha in order to further this objective.

Regarding Appellant's arguments with respect to Issue #1, Group #2 (claims 3, 13, and 21), it has been previously noted that the modification of system call jump tables is well-known in the art, both in the initial and final rejections. Appellant has made no attempt to contest this feature's status within the art, and has argued the Examiner's supporting evidence presented, Agarwal, is non-analogous art.

It is noted that the Microsoft Computer Dictionary, 5th Edition, in defining a "dispatch table," notes that the terms "dispatch table," " jump table," and "interrupt vector table" are synonymous with one another. Moreover, its definition of

"interrupt handler," the Microsoft Computer Dictionary, 5th Edition specifies that such interrupts invoke system functions, such as updating the system clock, and can be replaced by programmer-created handlers. These replacement handlers are installed by replacing the appropriate entry in the interrupt vector table.

The selection of particular data structures is generally not mentioned in disclosures in the genre of the instant application, as they reside at a lower layer in the programming structure that is beyond the scope of such specifications. Agarwal teaches to that lower layer, and discloses the loading of an interrupt vector table, which is a system jump table.

Regarding Appellant's arguments with respect to Issue #1, Group #3 (claims 7, 16, and 25), the same arguments regarding Issue #1, Group #1 apply to this group as well. No further explanation is necessary.

Regarding Appellant's arguments with respect to Issue #2, Group #1 (claims 4, 13, and 22), Appellant has argued that the Examiner has admitted that a prima facie case of obviousness has not been made. The Examiner is not aware of any such admission, and maintains that the case has been made, as stated in the final rejection.

Regarding Appellant's arguments with respect to Issue #2, Group #2 (claims 6, 15, and 24), Kernighan is merely used to further elaborate on the mechanism that would be used by Smaha and Epstein in the UNIX® environment

disclosed by Smaha, by describing the pertinent UNIX® systems calls that Smaha and Epstein would use. The stated motivation is sufficient.

Regarding Appellant's arguments with respect to Issue #3, Group #1 (claims 5, 14, and 23), Appellant's argument that the applied art is non-analogous.

It is noted that the Microsoft Computer Dictionary, 5th Edition defines a kernel as "the portion of the operating system that manages memory, files, and peripheral devices."

It has been disclosed that the invention of Smaha is used to detect system level events, as described above. Any mechanism that would perform such a task must necessarily modify the operating system in order to have the ability to be aware of system level events. Vu discloses such a mechanism for kernel modification for the purpose of detecting system level events that constitute misuses, thereby solving the problem of implementation in Smaha and Borchardt. The combination of Smaha, Borchardt, and Vu is therefore proper.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Matthew E. Heneghan
July 12, 2004

Conferees
Kim Vu
Gregory Morse

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120